

FILED

5/20/2021

CC

AO 106 (REV 4/10) Affidavit for Search
Warrant

AUSA Kaitlin Klamann, (312) 353-5361

THOMAS G. BRUON
CLERK, U.S. DISTRICT COURT

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION**

UNDER SEAL

21 CR 316

In the Matter of the Search of:

Case Number: 21 CR 316

The single-family home located at 1511 Guthrie Drive,
Inverness, Illinois, further described in Attachment A

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Holly Groff, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence, instrumentalities and contraband.

The search is related to a violation of:

Code Section

Offense Description

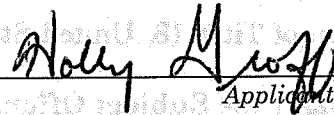
Title 18, United States Code, Sections 875(c), 2261A,
1591, 2422, 2252 and 2252A

Interstate threats; cyberstalking; sex trafficking of a
minor or by force, fraud, or coercion; enticement to
engage in prostitution; possession, receipt, and
distribution of child pornography

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.



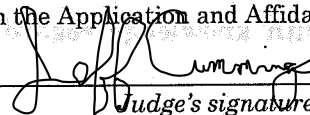
Applicant's Signature

**HOLLY GROFF, Special Agent
Federal Bureau of Investigation**

Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: May 20, 2021



Judge's signature

City and State: Chicago, Illinois

JEFFERY I. CUMMINGS, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Holly Groff, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been so employed since approximately June 2014. My current responsibilities include the investigation of criminal violations relating to sex trafficking, with an emphasis on sex trafficking of minors, in violation of Title 18, Unites States Code, Sections 1591, child exploitation and child pornography, in violation of Title 18, Unites States Code, Sections 2252, 2252A. I have received training in the area of sex trafficking, child pornography, and child exploitation.

2. This affidavit is made in support of an application for a warrant to search the single-family home located at 1511 Guthrie Drive, Inverness, Illinois 60010, Illinois, described further in Attachment A (the “**Subject Premises**”), for evidence, instrumentalities and contraband described further in Attachment B, concerning interstate threats, cyberstalking, sex trafficking and child pornography offenses, in violation of Title 18, United States Code, Sections 875(c), 2261A, 1591, 2422, 2252 and 2252A (“the **Subject Offenses**”).

3. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being

submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, and contraband of violations of Title 18, United States Code, Sections 875(c), 2261A, 1591, 2422, 2252 and 2252A, are located at 1511 Guthrie Drive, Inverness, Illinois.

I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

4. In or around March 2019, law enforcement began an investigation into MATTHEW SCHWARTZ after receiving multiple reports from the Illinois Department of Children and Family Services (DCFS) and Minnesota law enforcement related to a missing minor from Minnesota (“Minor A”) who was discovered in Illinois. During the course of the investigation, agents conducted numerous interviews with Minor A who provided information about Minor A’s and SCHWARTZ’s sexual relationship, including SCHWARTZ’s facilitation of Minor A’s travel from Minnesota to Chicago in order to engage in sex acts, SCHWARTZ’s recording of sex acts performed by Minor A, and SCHWARTZ’s payments to Minor A in exchange for sex acts performed by Minor A. During that investigation, agents also interviewed

SCHWARTZ's ex-girlfriend ("Individual A") who detailed a campaign of threats and harassment by SCHWARTZ against her following the break-up of their relationship.¹

5. As described in more detail below, there is probable cause to believe that evidence, instrumentalities and contraband of the **Subject Offenses** are located in the **Subject Premises**. Specifically, there is probable cause to believe that SCHWARTZ recorded sex acts with Minor A at the **Subject Premises** and such images are likely to be stored on electronic media at the **Subject Premises**. Additionally, there is probable cause to believe that SCHWARTZ utilized his cellular telephone to send threatening text messages to Individual A. Thus, there is probable cause to believe there is evidence, instrumentalities or contraband of the **Subject Offenses** on one or more cellular telephones belonging to SCHWARTZ located at the **Subject Premises**.

A. IDENTIFICATION OF THE SUBJECT PREMISES

6. According to Illinois to Secretary of State records, SCHWARTZ's driver's license lists the **Subject Premises** as his residence.

7. Based on surveillance and interviews of witnesses, law enforcement does not believe that any other individuals reside at the **Subject Premises**. Law

¹ On May 19, 2021, Magistrate Judge M. David Weisman signed a criminal complaint charging SCHWARTZ with interstate threats in violation of Title 18, United States Code, Section 875(c). *See* 21 CR 316 (under seal).

enforcement believes that SCHWARTZ has at least three children who either live independently elsewhere or with the children's mother, SCHWARTZ's ex-wife.

8. On or about December 3, 2020, SCHWARTZ sent an email to this Affiant from email address matt@nelix.com. The signature block of the email included the name "Matthew J. Schwartz" and listed the **Subject Premises** as his address.

9. As discussed in greater detail below, Buffalo Grove and Inverness Police Departments list the **Subject Premises** as SCHWARTZ's residence in reports of incidents involving SCHWARTZ.

B. SCHWARTZ MET MINOR A SEVERAL TIMES AT THE SUBJECT PREMISES TO HAVE SEX.

10. During the investigation, law enforcement conducted multiple interviews with Minor A. The interviews took place on or about March 14, 2019, May 25, 2019, October 16, 2019, and February 6, 2020, respectively. During the interviews, Minor A reported that she had a sexual relationship with MATTHEW SCHWARTZ. Specifically, and among other things, Minor A stated that she had sex with MATTHEW SCHWARTZ at the **Subject Premises** and that MATTHEW SCHWARTZ recorded sex acts with Minor A on his phone.

1. March 14, 2019 Interview with Minor A

11. On or about March 14, 2019, Buffalo Grove Police Department interviewed Minor A² following a 911 call placed by Minor A to the Buffalo Grove

² Minor A is not receiving any benefit for providing information to law enforcement.

Police Department. That interview was recorded and I reviewed a copy of the recording. Minor A told law enforcement that she met SCHWARTZ over Facebook in approximately July 2018. Minor A stated that her Facebook page is under her name and SCHWARTZ's Facebook page is under his full name. According to Minor A, SCHWARTZ sent her a Facebook friend request. Minor A and SCHWARTZ began to talk over Facebook and e-mail and shortly after, met in person.

12. Minor A stated that she had sex with SCHWARTZ and spent time with him. In exchange, SCHWARTZ gave her a place to stay, a car, paid her cell phone bill and gave her money every month. Specifically, Minor A stated that SCHWARTZ paid her \$5,000 a month. Minor A stated that SCHWARTZ would frequently pay her in cash. Minor A stated that the last time she had sex with SCHWARTZ was less than a week prior to the interview with law enforcement. Minor A stated that she has previously had sex with SCHWARTZ at his home in Buffalo Grove, as well as his home in Inverness (**the Subject Premises**). Minor A estimated that she had sex with SCHWARTZ at least once a week. According to Minor A, SCHWARTZ recorded sex acts with Minor A on Minor A's phone and on SCHWARTZ's phone. Minor A told agents she couldn't recall SCHWARTZ's full phone number but she stated that it ended with the numbers 1591³.

³ According to AT&T records, phone number (224) 520-1591 ("Schwartz Phone 2") is subscribed to Nelix Inc. at the **Subject Premises** with a contact name of "Matt Schwartz."

13. At the time that Minor A was initially contacted by SCHWARTZ, Minor A was sixteen years old. Minor A stated that she initially lied to SCHWARTZ about her age, telling SCHWARTZ she was twenty years old. According to Minor A, SCHWARTZ eventually found out her real age when he saw her driving permit. After that, SCHWARTZ didn't speak to her for about a week but eventually reached out and wanted to see her again.

14. At the time that she met SCHWARTZ, Minor A told law enforcement she was in a romantic relationship with a man who lived in Chicago ("Individual B"). Minor A continued to date Individual B until approximately one month before the interview. In or around December 2018, Minor A asked SCHWARTZ to buy a car for her. SCHWARTZ gave Minor A \$60,000 to buy a Porsche. According to Minor A, Minor A and Individual B flew to North Carolina and bought a 2016 Porsche Macan. Minor A asked Individual B to register the car in his name and turn over the Porsche to Minor A when she turned 18. Instead, Individual B kept the Porsche and never gave it to Minor A.

15. According to records obtained from Allstate Insurance Co., a 2015 Porsche Macan was insured by SCHWARTZ during the month of September 2019.

16. Minor A also told law enforcement that at some point, SCHWARTZ rented her a car. Minor A said that Individual B wrecked the rental car. According to records obtained from Hertz rental car company, SCHWARTZ rented a 2018 Malibu with Missouri license plate BA9K4D ("Rental Car 1") from Chicago O'Hare

International Airport on or about February 23, 2019. According to reports obtained from the Illinois State Police, Minor A was involved in a traffic crash on February 25, 2019 while driving Rental Car 1.

17. Approximately one month before the interview, Minor A stated that DCFS came and took her back to Minnesota. Two weeks later, SCHWARTZ bought Minor A a plane ticket to fly back to Chicago. Minor A said she arrived in Chicago on or about March 11, 2019.

18. Minor A stated that she had been at SCHWARTZ's house (the **Subject Premises**) the night before the interview and that she and SCHWARTZ had gotten into an argument. Minor A stated that SCHWARTZ called the Inverness Police Department and reported that Minor A had stolen his cell phone. Minor A told law enforcement that SCHWARTZ had given her the cell phone to use while she waited for delivery of a new phone. Minor A was contacted by the police telling her she had to return the phone to the Inverness Police Department by 10:00 p.m. on the day of the interview.

19. According to an Inverness Police Department report, Inverness Police Department received a 911 call from SCHWARTZ about a domestic incident on or about March 13, 2019 at approximately 11:00 p.m. at the **Subject Premises**. SCHWARTZ is listed as the complainant on the report. According to the report, SCHWARTZ told officers that Minor A was his ex-girlfriend and that she took two of his cell phones during an altercation. According to the report, SCHWARTZ provided

officers with a false last name for Minor A. Minor A told the officer that she only took one phone from SCHWARTZ. The officer informed Minor A that she needed to return the phones to the officer at the Inverness Police Department. Minor A also provided Inverness police officers with her phone number. According to the report, after the interviews, Inverness PD ran the telephone number provided by Minor A through law enforcement databases and discovered her real identity as a missing minor from Minnesota.

20. According to Minor A, after she left the **Subject Premises** at 3:00 a.m. the morning of the interview, she had pulled over in a parking lot to sleep. Minor A woke up and SCHWARTZ was there with another woman (“Individual C”). According to Minor A, SCHWARTZ had a knife and Individual C had a taser. SCHWARTZ and Individual C demanded the return of SCHWARTZ’s cell phone. Victim A called 911 but SCHWARTZ left the area with the cell phone before police arrived. Minor A stated that SCHWARTZ was arrested for domestic battery later that day as a result of a report Minor A filed regarding the incident.

21. According to records obtained from the Buffalo Grove Police Department, officers responded to the parking lot of a Walgreens regarding a domestic battery incident on March 14, 2019 at approximately 7:54 a.m. According to the report, Minor A reported that she was attacked by SCHWARTZ while she was seated in her vehicle. Minor A stated that SCHWARTZ demanded his cell phone be returned and threatened her with a kitchen knife. Individual C had driven

SCHWARTZ to the Walgreen's parking lot. Individual C threatened Minor A with a "taser-like" device. SCHWARTZ retrieved his cell phone from Minor A and then left the scene with Individual C. The report states that Buffalo Grove PD requested that the Inverness Police Department respond to the **Subject Premises** to take SCHWARTZ into police custody relative to domestic battery charges.

2. May 25, 2019 Interview of Minor A

22. On or about May 25, 2019, FBI agents spoke with Minor A via telephone. During the interview, Minor A provided additional details related to how she met SCHWARTZ. She stated that she accepted SCHWARTZ's friend request on Facebook and the two engaged in a conversation on Facebook for approximately two days. SCHWARTZ and Minor A then agreed to meet in person. At their first meeting in or around July or August 2018, Minor A told SCHWARTZ she was looking for someone that could provide her with financial support. SCHWARTZ told Minor A that he was looking for a sugar baby or a girl he could have sex with for money, but not have any emotional attachments with her. SCHWARTZ also wanted to be able to have relationships with other girls.

23. Minor A also provided agents with additional background information regarding her relationship with SCHWARTZ. Specifically, Minor A told agents that SCHWARTZ gave Minor A \$400 the first time they met. SCHWARTZ also gave her \$400 the second time they met. The third time they met, Minor A stated that SCHWARTZ made a comment that he wasn't paying Minor A to just meet and

hangout. Minor A understood SCHWARTZ to mean that he would stop paying her if she did not have sex with him. So Minor A had sex with SCHWARTZ for the first time during this visit. SCHWARTZ then offered to pay Victim A \$4,000 a month to continue their relationship. Starting in August of 2018, SCHWARTZ paid Minor A \$2,000 every two weeks. In return, Minor A would come to his house one to three times a week and have sex with him. Minor A understood that SCHWARTZ could afford to pay her these amounts because he had just sold his company for between \$6-8 million. Later, Minor A asked SCHWARTZ to pay her \$5,000 a month and he agreed.

24. Minor A said that she believes SCHWARTZ found out she was sixteen years old sometime near the end of 2018. At that time, SCHWARTZ found Minor A's driving permit and determined her age. SCHWARTZ also found out that Minor A was an underage missing person from Minnesota by searching her name on the Internet.

25. Minor A stated that while in Minnesota, she used a relative's phone ("Relative Phone 1") to contact SCHWARTZ. According to Minor A, SCHWARTZ told Minor A he didn't care if she was sixteen and that he wanted to continue their relationship. SCHWARTZ then sent money to Minor A so she could buy a plane ticket back to Chicago. Minor A bought the ticket and returned in February 2019. Minor A stated that SCHWARTZ still gives her money, but not as regularly.

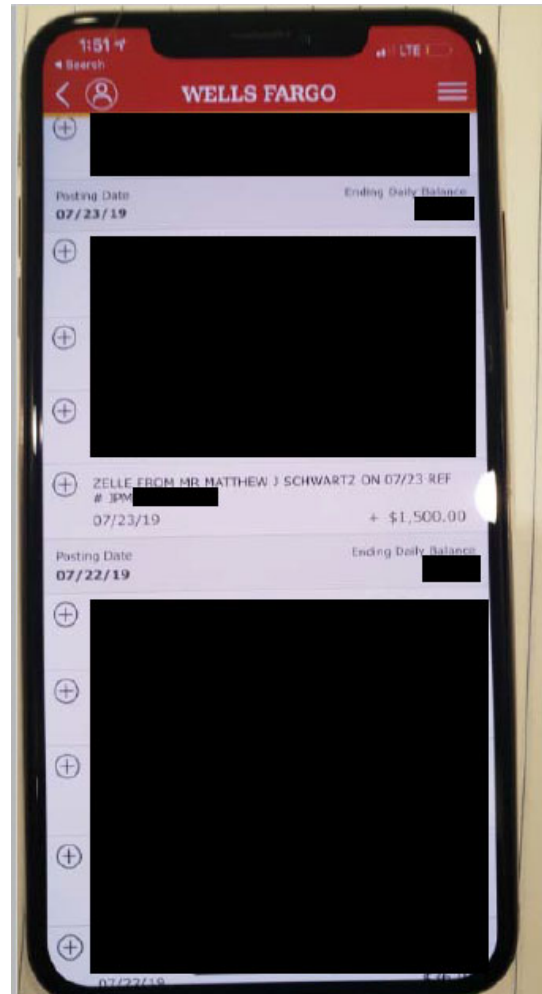
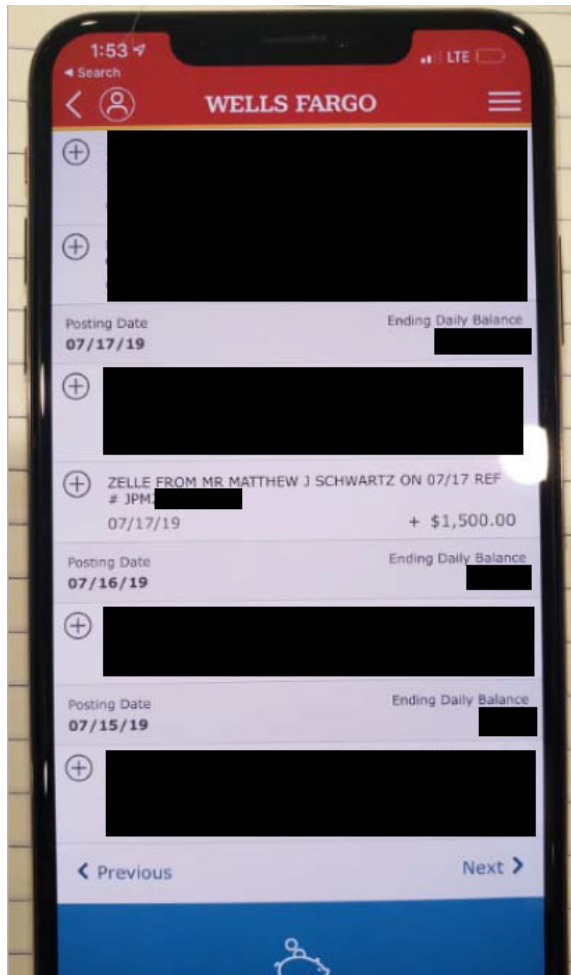
3. *October 16, 2019 Interview of Minor A*

26. On or about October 15, 2019, agents received a phone call from Minor A. Minor A told agents that she met with SCHWARTZ earlier the same day at the **Subject Premises**. SCHWARTZ and Minor A argued. Minor A found out that SCHWARTZ had been in contact with other girls who were Minor A's age (minors). Minor A believed SCHWARTZ was having a sexual relationship with at least one other minor. During the argument with SCHWARTZ, Minor A called 911. Police officers subsequently arrived at the **Subject Premises**.

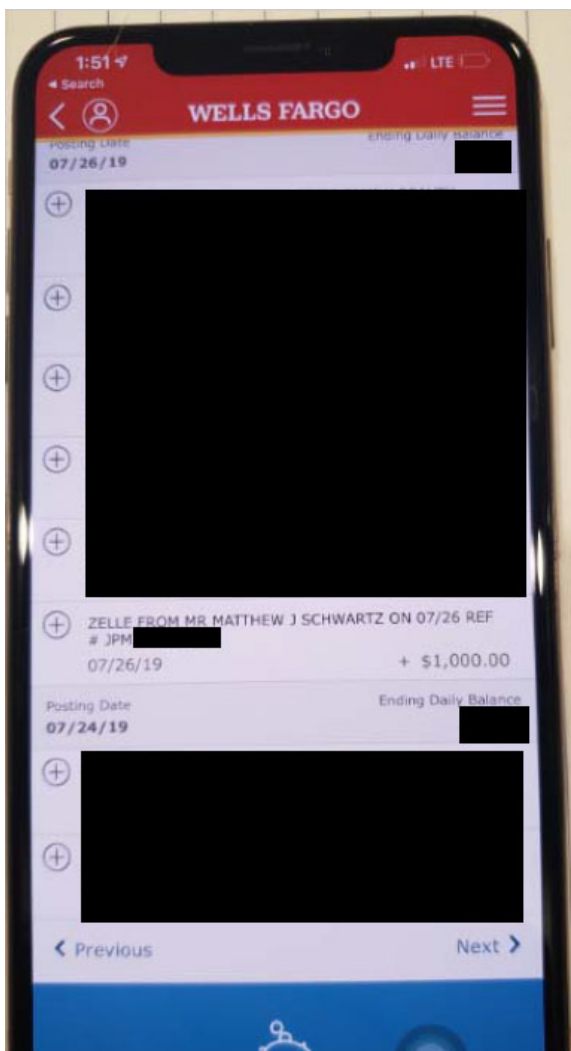
27. On or about October 16, 2019, FBI agents met with Minor A at an auto store at the request of Minor A. Minor A told agents that she was at the auto store because her newly purchased vehicle needed maintenance. FBI agents conducted an in-person interview with Minor A at a nearby Starbucks café. Minor A stated that she continued to see and have sex with SCHWARTZ after her interview with FBI in May 2019. Even though she was sent back to Minnesota, she was frequently in touch with SCHWARTZ and SCHWARTZ frequently paid for airline tickets for Minor A to travel to Chicago. Minor A usually purchased airline tickets through American Airlines and Delta Airlines. SCHWARTZ also traveled to Minnesota on occasion to visit Minor A.

28. SCHWARTZ continued to pay Minor A approximately \$5,000 a month. Minor A agreed to see SCHWARTZ twice a month for \$2,500 per visit. Minor A stated SCHWARTZ often paid her in cash but would also transfer money to her bank account via Zelle. Minor A showed agents records of deposits from SCHWARTZ on a Zelle

application on her phone. Below are photographs of Minor A's phone⁴ depicting payments from SCHWARTZ in the amount of \$1,500 on or about July 17, 2019 and July 23, 2019 and in the amount of \$1,000 on or about July 26, 2019:



⁴ Certain information was redacted from these images to protect Victim A's privacy.



29. According to records obtained from Early Warning Services (the parent company of Zelle), five monetary payments were made to Minor A by SCHWARTZ between on or about July 18, 2019 and on or about August 5, 2019. The total amount of money paid by SCHWARTZ to Minor A during these transactions was approximately \$5,250. At the time of these transactions, Minor A was 17 years old.

30. According to records obtained from MidWestOne bank, three wire transactions were made to Minor A's account by SCHWARTZ or Nelix, Inc. between

on or about September 26, 2019 and on or about March 5, 2020. The total amount of money paid by SCHWARTZ and Nelix, Inc. to Minor A during these transactions was approximately \$24,100.

31. Database checks and open source information indicate that MATTHEW SCHWARTZ was the President of the company NELIX, INC, an internet development firm.

32. Minor A also told agents that she communicated with SCHWARTZ by contacting him on his cell phone. Minor A provided his cell phone number as (847) 682-6054 (“Schwartz Phone 1”)⁵. Minor A stated that she had blocked SCHWARTZ on her cell phone and deleted all of the text messages they exchanged.

33. Minor A stated that she also communicated with SCHWARTZ over email. Minor A showed agents some of the emails that she exchanged with SCHWARTZ and allowed agents to take screen captures of the communications. Below is a photograph of Minor A’s cell phone which displays one of the emails with SCHWARTZ that Minor A showed agents⁶:

⁵ According to AT&T records, phone number (847) 208-8064 (“Schwartz Phone 1”) is subscribed to Nelix, Inc. at the **Subject Premises** with a contact name of “Matt Schwartz.”

⁶ Certain identifying information is redacted from the photograph.



34. Minor A told agents that the above exchange took place on or about August 28, 2019 and the email pertained to her breast reduction surgery. Minor A recalled that during the time of the email communications, SCHWARTZ was enrolled in a drug rehab facility located in Florida. At this time, Minor A was 17 years old.

35. Minor A stated that she flew from Minnesota to Chicago the day before the interview. Minor A said SCHWARTZ bought her ticket. Minor A planned to buy a car while she was in Chicago and stated that SCHWARTZ had agreed to co-sign the loan.

36. Minor A stated that after she landed at O'Hare airport, she took an UBER to the **Subject Premises**.

37. According to records obtained from UBER, a trip was made through the UBER account associated with Minor A's telephone number on or about October 15, 2019 at 10:35 a.m. from the area of Chicago O'Hare International Airport to the **Subject Premises**.

38. Additionally, UBER records show a number of trips on Minor A's account to or from the **Subject Premises** in the days before the altercation on October 15, 2019. For example, the records show the following trips:

a. on or about October 11, 2019, with a pick-up at approximately 12:42 p.m. at the **Subject Premises** and a drop-off location in Hickory Hills, Illinois at 1:35 p.m.;

b. on or about October 11, 2019, with a pick-up at approximately 5:08 p.m. at a location in Chicago, Illinois and a drop-off location at the **Subject Premises** at 6:26 p.m.; and

c. on or about October 12, 2019, with a pick-up at approximately 9:02 p.m. at the **Subject Premises** and a drop-off location in Wood Dale, Illinois at 9:31 p.m.

39. Minor A stated that SCHWARTZ was upset with Minor A when she arrived at the **Subject Premises**. According to Minor A, SCHWARTZ said that another woman was on her way to his house and SCHWARTZ didn't want Minor A

to be there when the woman arrived. Minor A and SCHWARTZ argued. Minor A called 911 but hung up before dispatch answered. SCHWARTZ then left the **Subject Premises** and took Minor A's cell phone with him when he left. After SCHWARTZ left, officers with the Inverness Police Department arrived. According to Minor A, the officers gave Minor A a ride to Elk Grove Village, Illinois.

40. According to Inverness PD reports, on October 15, 2019, Individual C called 911 to report an unwanted person at the **Subject Premises**. Individual C informed law enforcement that she worked for SCHWARTZ and that Minor A refused to leave the **Subject Premises**. Upon law enforcement's arrival, Individual C stated that Minor A had arrived at the **Subject Premises** by UBER. Individual C explained that she knew Minor A as someone who SCHWARTZ was attempting to assist in life. SCHWARTZ and Minor A got into a verbal altercation. SCHWARTZ left the **Subject Premises** to obtain an Order of Protection related to the verbal altercation with Minor A. Individual C requested that Minor A leave the **Subject Premises**, but Minor A refused to leave the **Subject Premises**. Law enforcement conducted a search of the **Subject Premises** and located Minor A hiding in a darkened closet in the basement.

41. According to the Inverness PD report, Minor A stated to law enforcement that she had an on and off relationship with SCHWARTZ and that he was assisting her financially. Minor A stated that for approximately one year, SCHWARTZ has been flying Minor A to Chicago from her residence in Minnesota.

Minor A stays with SCHWARTZ for a few days and then travels back to Minnesota. Minor A explained that she arrived at the **Subject Premises** by UBER. Soon after arriving, she and SCHWARTZ got into a verbal argument. SCHWARTZ left the **Subject Premises** as he was angry with Minor A. Minor A then got into an argument with Individual C.

42. According to Inverness PD reports, law enforcement contacted SCHWARTZ.⁷ The phone number listed on the Inverness PD report for SCHWARTZ is Schwartz Phone 1. SCHWARTZ confirmed that he had a verbal altercation with Minor A. SCHWARTZ denied purchasing an airline ticket for Minor A to travel to Chicago, insisting that Minor A showed up to the **Subject Premises** unannounced. SCHWARTZ agreed to provide his credit card number to Individual C so that she could buy an airline ticket for Minor A back to Minnesota in order to get Minor A out of SCHWARTZ's life. Inverness PD reports state that Minor A was initially amenable to accepting the return flight back to Minnesota, however Minor A changed her mind and requested to be transported to Elk Grove Village, Illinois. Minor A was transported to Elk Grove Village and law enforcement observed Minor A to be picked up by a vehicle.

⁷ A previous affidavit submitted in support of a search warrant for Facebook Account ID 1275748805 stated that the report stated officers contacted SCHWARTZ by telephone. *See* 20 M 270. The report does not specify the method of communication used to contact SCHWARTZ.

43. Minor A stated that approximately one week prior to the interview with agents, SCHWARTZ told her he was going to “cut off some girls” and that he was tired of giving out money. SCHWARTZ agreed to pay Minor A a lump sum payment of \$30,000 signifying \$5,000 payments made each month for six months as severance pay for “cutting her off”. Minor A also told agents that she has automobile insurance coverage through SCHWARTZ’s auto policy.

44. According to Allstate Insurance records, SCHWARTZ included Minor A as a driver on his auto policy beginning in or around September 2019 through in or around October 2019.

45. On October 16, 2019, after the conclusion of the interview with Minor A, Minor A contacted agents and informed them that she had received the below email from SCHWARTZ. Minor A stated she felt threatened by the email she received from SCHWARTZ, via email address ‘matt@nelix.com.’ Minor A forwarded the email to FBI agents for possible further investigation. Minor A explained that the email made reference to a vehicle she had just purchased.

On Wed, Oct 16, 2019 at 3:17 PM Matthew Schwartz <matt@nelix.com> wrote:

The dealership has you noted for Fraud, and they will never do business with you again. Additionally they are putting you on a global list that many dealerships reference Good luck getting a car, for the rest of your life.

WOW, you stole a shit ton from me. My colognes, Adriana's perfumes lotions, that bracelet, airpods, clothing. Some of it you admitted to in texts. As for the rest - I have camera's everywhere you know. Shit for brains.

And I KNOW that you took the radar detector, the apple watch, the \$3K you blamed on Amanda and / or Dezzy. You are a giant piece of shit. You even look like one. You smell like one too. I didn't mention it because I was being nice.

You know, assholes your age can be prosecuted as adults when they commit as many crimes as you have.

Do you think anybody is going to believe your lies? OMG I have so much shit against you, the fact that every word out of our mouth is complete and utter bullshit will be evident within 5 minutes in any court of law. I guarantee you. WOW

No need for a reponse. I'm blocking you via e-mail right now. Have a fucked up life mental midget.

Matt

4. February 6, 2020 Interview with Minor A

46. On or about February 2, 2020, FBI was notified by an officer with the North Riverside Police Department that Minor A was in police custody. Later, the officer contacted FBI and informed agents that Minor A was released to the Illinois Department of Family and Child Services.

47. On or about February 6, 2020, agents spoke to Minor A by phone. Minor A stated that she continued her relationship with SCHWARTZ since last speaking with agents. Minor A stated that instead of paying her in money, SCHWARTZ pays

her with expensive gifts. According to Minor A, SCHWARTZ would send her gifts in the mail or buy her gifts when they are together. Gifts include purchases from the PINK store, purses and payments for hotel stays. Minor A said she now meets with SCHWARTZ approximately once every two months.

48. Minor A drove from Minnesota to Chicago on or about January 30, 2020 to meet SCHWARTZ. Prior to driving to Illinois, Minor A dropped a friend ("Minor B") off at Minor B's boyfriend's house in Minnesota. Minor A then drove to Illinois and met SCHWARTZ at a Hilton Garden Inn located in Des Plaines, Illinois. SCHWARTZ met her at the hotel and rented a hotel room. According to Minor A, SCHWARTZ did not spend the night in the hotel with her.

49. According to Minor A, Minor B and Minor B's boyfriend arrived at the hotel the following day. Minor A asked SCHWARTZ to rent a hotel room for them and he agreed. Minor A stated that Minor B had never met SCHWARTZ before and that Minor B did not have sex with SCHWARTZ. According to records obtained from the Hilton Garden Inn O'Hare, SCHWARTZ booked two hotel rooms at the Hilton Garden Inn O'Hare via an online platform on or about January 30, 2020 for two nights. The hotel records further reflect that the reservation for both rooms was extended for two additional nights, with a check-out date of February 3, 2020. SCHWARTZ provided the **Subject Premises** as his address, email address matt@nelix.com, and the number for Schwartz Phone 1 to the hotel to secure the reservation.

50. Agents reviewed the available surveillance footage of the lobby of the Hilton Garden Inn O'Hare taken on or about January 30, 2020 and observed the following:

a. At approximately 5:56 p.m., an adult male matching the appearance of SCHWARTZ based on a review of his Illinois driver's license photograph and Facebook account, approached the front desk of the Hilton Garden Inn O'Hare and appeared to hand over an identification card to the front desk employee. SCHWARTZ then swiped a card through the card reader at the front desk. The front desk employee handed what appeared to be room keys to SCHWARTZ. SCHWARTZ then exited the hotel through the front entrance.

b. At approximately 6:03 p.m., SCHWARTZ reentered the hotel carrying multiple bags and placed the bags on a bell hop cart. SCHWARTZ pushed the bell hop cart through the lobby and around the front desk.

c. At approximately 6:16 p.m., two unknown female entered the hotel lobby from the exterior and walked by the front desk. One of the female was carrying multiple bags and rolling a suitcase.

51. Agents also reviewed the surveillance footage from the Hilton Garden Inn taken on or about February 1, 2020 and observed the following:

a. At approximately 4:46 a.m., SCHWARTZ entered the hotel vestibule.

b. At approximately 5:53 a.m., SCHWARTZ stood at the front desk with an unknown female. SCHWARTZ appeared to hand the front desk employee hotel keys. The front desk employee subsequently handed hotel keys back to SCHWARTZ. SCHWARTZ then appeared to hand a hotel key to the unknown female.

c. At approximately 6:03 a.m., SCHWARTZ departed the hotel.

52. According to Minor A, on or about February 2, Minor A, Minor B and Minor B's boyfriend went shopping in North Riverside, Illinois. Minor A told agents that employees at one store believed they were shoplifting and called the police. Responding law enforcement discovered that both Minor A and Minor B were under the care of the state of Minnesota. Minor A and Minor B were flown back to Minnesota on or about February 5.

C. SCHWARTZ SENT TEXT MESSAGES FROM THE SUBJECT PREMISES TO HARASS AND THREATEN INDIVIDUAL A.

53. On or about November 9, 2020, a 22-year-old female ("Individual A") was interviewed by law enforcement regarding, among other things, her relationship with her ex-fiancé, MATTHEW SCHWARTZ. Individual A met SCHWARTZ online in the summer of 2018. At that time, Individual A was 20 years old and SCHWARTZ was 48 years old. Individual A and SCHWARTZ entered into an arrangement under which Individual A provided companionship to SCHWARTZ in exchange for monetary payment. Later, SCHWARTZ developed romantic feelings for Individual A and the two became engaged to be married in September 2019. Approximately four months

later, in February 2020, Individual A ended the engagement. Soon thereafter, SCHWARTZ began a campaign of threats and harassment against Individual A.

54. Specifically, beginning in or around May 2020, Individual A began to receive text messages from unknown phone numbers. As described below, investigators determined that each of the unknown phone numbers was created using a mobile application called the Burner App and Schwartz Phone 1 was the number associated with each of the Burner App phone numbers that contacted Individual A.

1. May 31, 2020 Text Messages

55. On or about May 31, 2020 at approximately 1:00 a.m., Individual A received several text messages from phone number (815) 255-3591 (“Burner Phone 1”). The first text message stated, “I am going to attack the fuck out of you and kill you dead if you do not start talking to me I’m not fucking kidding. What you did to me was atrocious motherfuckers will kill for \$10,000 what you did to me with 300 fucking thousand dollars two years of my life and my worst fucking nightmare you deserve to be choked life are you do you need to come talk to me or things are gonna get really fucking bad I’m going to prison anyway bitch so who the fuck cares right I got another [nothing] left to lose.” The next text message, sent on the same day and time, read, “Honestly deaths too good for you.” The next text message stated, “Give me the phone number [of] your sugar daddy so I can talk to [him] [re]member when you we’re [were] gonna do that you never did.” The following text message stated, “So he could pay me off and make [male name] you tell him to come your fucking check

now I'll check tell him to wire transfer \$300,000 and I will leave you the fuck alone you'll never hear form me again you know what let's make it 350 for pain and suffering three and \$50,000 and you'll never have to hear from me again good at 350000".

56. On or about February 24, 2021, law enforcement obtained records from Ad Hoc Labs, Inc., the developer of Burner, a mobile application which generates temporary disposable phone numbers. According to Ad Hoc Labs records, Burner Phone 1 was created on May 31, 2020 and expired on June 14, 2020. Ad Hoc Labs records indicated that Schwartz Phone 1 was the "user phone number" for Burner Phone 1.

57. According to records obtained from AT&T, the financially liable party for Schwartz Phone 1 is Nelix Inc, with listed contact name as Matt Schwartz with a user address of the **Subject Premises**.

58. Additionally, as discussed above, on or about December 3, 2020, this Affiant received an e-mail from email address matt@nelix.com that was signed by MATTHEW SCHWARTZ. The email signature block read "Matthew J. Schwartz CEO Nelix, Inc." and the email included the number for Schwartz Phone 1 at the end of the message.

59. On or about May 5, 2021, I had a telephone call with a representative of Ad Hoc Labs who explained that the "user phone number" reflected in Ad Hoc Labs records is the phone number entered by a user during the creation of an account with

Burner App. The representative further explained that after a user enters a phone number into the Burner App, a verification code is sent to that phone number that must be entered into the Burner App by the user in order for the user to create a Burner account and subsequently create a Burner Phone number.

2. November 3, 2020 Text Messages

60. On or about November 3, 2020 at approximately 2:41 a.m., Individual A received several text messages from phone number (217) 803-7845 (“Burner Phone 2”). The first text message stated, “Hey bitch. It really irritates me. That you blocked me again. You know how pointless it is right?” The next text messages stated, “You know the endgame is designed so that you don’t get hurt. And in fact it ends up with you in a good place. I can change that. So that it ends with you getting ended. And I could end with you getting ended in one of three ways. 1) quick and painless. 2) slow and painful 3) a kind of living death. But I chose option 4) you not getting ended at all. Instead you are left actually in a better place. You see? I love you. And that is why. But don’t push me. . . . Just be happy I’m taking the high road and not hurting you. Most people would choose a different path. Don’t fuck with me or I will become most people. I will choose #2 instead of #4. Don’t be dumb I really don’t want to hurt you that way. I don’t want to do #1, 2, 3. Don’t make me. Don’t fuck me up. Don’t antagonize me. It would be really dumb. And by the way, what I got planned is completely independent on [of] me, and if anything happens to me it will escalate and get way worse, putting your family in danger and all fingers will point at you. Also I

have an opportunity, to do something really really bad tonight – something that would fuck you up really hard. But I have passed on the opportunity. You are welcome. Because I love you. So I’m holding back You have a lot of enemies though. One of them may [take] the opportunity, but it won’t be me.”

61. According to Ad Hoc Labs records, Schwartz Phone 1 was the “user phone number” for Burner Phone 2. Burner Phone 2 was created on November 3, 2020 and expired on November 11, 2020.

3. November 27, 2020 Text Messages

62. On or about November 27, 2020 at approximately 2:10 a.m., Individual A received several text messages from phone number (312) 219-3639 (“Burner Phone 3”). The first message stated, “Seriously I know of 2 other guys who had a girl like you who did the same thing to them that you did to me. One of them killed themselves. One of them killed the girl. What would you have done if you were me? Seriously. Think about it all. Not just one isolated incident. But every bit of it start to finish. Put yourself in my place and imagine how it feels. . . . I should have just killed you. But I couldn’t live with myself. And now the best choice is for me to kill myself. I bet you won’t care. Or worse. You’ll be Fucking happy about it. Evil. Sick. Horrible. I can’t even believe you were somebody I once thought had good qualities. Fuck I was so wrong.” The next text message stated, “And now you just ignore me. You think that will make me go away. It just strengthens my resolve. If I decide to kill my self – and

I'm close to that decision. You could be damn sure I'll be taking you and your flavor of the day with me."

63. According to Ad Hoc Labs records, Schwartz Phone 1 was also the "user phone number" for Burner Phone 3. Burner Phone 3 was created on November 27, 2020 and expired on November 30, 2020.

64. In addition to Burner Phone 1, Burner Phone 2, and Burner Phone 3, Ad Hoc Labs records indicated that Schwartz Phone 1 was listed as the "user phone number" for at least 12 additional disguised phone numbers created using the Burner App between approximately May 31, 2020 and December 1, 2020.

65. According to records obtained from Apple, the Burner App was downloaded by Apple ID account nelix@me.com subscribed to by SCHWARTZ ("Schwartz Account 1") on or before February 20, 2020. The Apple records show the Burner App was updated or redownloaded by Schwartz Account 1 numerous times between February 2020 and March 2021.

66. Additionally, Apple records indicate that Schwartz Account 1 made several purchases of "credit packs" and Burner monthly subscriptions from Ad Hoc Labs beginning in or around March 2020 until approximately March 2021. According to a representative from Ad Hoc Labs Inc., a user of the Burner App must purchase credit packs or subscriptions in order to make and receive phone calls and send and receive text messages from Burner phone numbers.

67. According to Apple records, Schwartz Account 1 purchased several credit packs and monthly subscriptions from Internet Protocol (“IP”) address 24.1.179.253. According to records obtained from Comcast, as of at least October 3, 2020, IP address 24.1.179.253 was subscribed to SCHWARTZ at the **Subject Premises**.

D. IDENTIFICATION OF A SEX ROOM AT THE SUBJECT PREMISES

68. In or around April 2021, law enforcement obtained records from Ring LLC, a home security and smart home company owned by Amazon. According to Ring records, SCHWARTZ owns several Ring devices that are installed at the **Subject Premises** including a “Chime pro” device which was assigned the description “CHIME Sex Room.” According to Amazon.com, a Ring Chime Pro is a “three-in-one solution that includes a wifi extender for your Ring cameras and doorbells, a nightlight, and a chime box to hear notifications for your Ring cameras and doorbells.” According to Amazon.com, the device allows the user to “hear real-time notifications when your connected cameras and doorbells detect motion, or when someone rings your doorbell.”

69. In or about May 2021, law enforcement spoke to Individual A. According to Individual A, SCHWARTZ has a “sex room/secret room” at the **Subject Premises**. According to Individual A, the sex room is located on the second floor of the residence. The room has two entry points, one through the closet in the bathroom and the second through a secret entry point behind a bookshelf. The residence is a “smart home” and

is controlled through the Alexa Application. The sex room and closets in **Subject Premises** are capable of being locked/unlocked through the Alexa App. SCHWARTZ keeps his sex toys and women's clothing; to include shoes and wigs in the sex room. Individual A has had sex with SCHWARTZ in the sex room. SCHWARTZ took naked photographs of Individual A without her knowledge. Individual A discovered the photographs on one of SCHWARTZ's cell phones.

E. SCHWARTZ SENDS TEXT MESSAGES CONTAINING "DISTURBING MESSAGES" ON MAY 15, 2021.

70. On or about May 16, 2021, the Affiant received a telephone call from Robert Haas, the Chief of Police at the Inverness Police Department. In summary, Chief Haas informed the undersigned that he received a tip from an individual ("Individual D") who claimed to be an acquaintance of SCHWARTZ that SCHWARTZ was making disturbing statements to Individual D. Individual D provided Chief Haas with screenshots of text messages that Individual D claimed came from SCHWARTZ on or about May 15, 2021. Chief Haas sent those screenshots to the Affiant. At the top of the screen depicting the conversation, there is a small circle with a photograph in it and the letter "m" next to it. Based on my training and experience and my experience using mobile devices, I believe these items are identifiers for a mobile contact. In this instance, the photograph depicts a middle age white male in a collared shirt and tie. I compared this photograph with SCHWARTZ's digital driver's license

image and images on his Facebook profile. Based on that comparison, I believe the individual depicted in this photograph is SCHWARTZ.

71. The text messages included the following statements: “I don’t know its come to this;” “Covid killed Nelix [SCHWARTZ’s company];” “I don’t know how its come to this. So yeah a killing spree/suicide is sounding pretty good these days;” “I pissed way 6 million dollars on. 2.5 years. Ha Ha. About a million of it was stolen or finessed. By various people. A million to bad investments. A million to debt. A million to drugs and virus. A million to my house and car. A million to everything else.... Kids. College. Two cruises. Tons of girls clothing shoes and wigs. Etc etc etc. I’ve got about half a million left but its locked up and o [I] can’t touch it;” “I hate life;” “I hate me;” “I hate everything;” “I’m having a hard time;” “I don’t know what to do;” and “I can’t find the answer.”

II. BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

72. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways:

73. Those who create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create video and still images, including most cellular telephones and Personal Digital

Assistants (“PDA”) (*e.g.*, a Blackberry). Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device’s memory card directly onto the computer or into a storage account accessible from any computer with the capability of accessing the internet (sometimes referred to as a “cloud” account). Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones, as well as other computers. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

74. The computer’s capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media, such as floppy disks, also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child

pornography search warrants often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

75. My training and experience, and the training and experience of other agents whom I have consulted, have shown the following:

a. The majority of individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals almost always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

b. Possessors, traders and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts. Therefore, any records, documents, invoices and materials in any format or medium that concern online storage or other remote computer storage could indicate that a person at the Subject Premises is storing illegal material in an online storage account.

III. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

76. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an

electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

77. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

78. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

79. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads, including Schwartz Phone 1 and Schwartz Phone 2 offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") or facial recognition in lieu of a numeric or alphanumeric passcode or password.

80. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints, either their own or others', that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device.

81. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include when more than 48 hours have passed since the last time the device was unlocked. The Touch ID feature will also not work and entry of a passcode will be required if the device's user or someone acting on the user's behalf has remotely locked the device. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID, and execute the search authorized by the requested warrant, exists only for a short time (*i.e.*, 48 hours or less, or until the device is given a remote lock command). Touch ID also will not work to unlock the device if the device has been turned off or restarted (*e.g.*, if the device's battery becomes fully depleted), or after five unsuccessful attempts to unlock the device via Touch ID are made. In addition, I also know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as

iPhones and iPads offers users the ability to remotely erase the contents of such devices.

82. If a user enables facial recognition access on a given device, a user may enable the device to be unlocked using his face. For example, this feature is available on certain Apple devices and is called “Face ID.” During the Face ID registration process, the user holds the device in front of his face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly.

83. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

84. As discussed in this affidavit, based on my training and experience I believe that SCHWARTZ possesses Schwartz Phone 1 and Schwartz Phone 2. The passcodes or passwords that would unlock the phones are not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access

the data contained within the phones, making the use of biometric features necessary to the execution of the search authorized by this warrant.

85. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, Apple devices allow only five unsuccessful match attempts before a passcode is required. A user must enter the passcode for additional security validation when: the device has just been turned on or off, the device has not been unlocked for more than 48 hours, the passcode has not been used to unlock the device in the last six and a half days and Face ID has not unlocked the device in the last 4 hours, the device has received a remote lock command, and after initiating power off/Emergency SOS. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

86. As described in Attachment A, Schwartz Phone 1 and Schwartz Phone 2 are Apple brand devices, specifically Schwartz Phone 2 is an Apple iPhone 8 Plus and Schwartz Phone 1 is an Apple iPhone 11 Pro Max. According to Apple's website, model iPhone 8 Plus supports Touch ID⁸ and model iPhone 11 Pro Max supports Face ID.⁹

87. As discussed above, SCHWARTZ has been identified as the user of Schwartz Phone 1 and Schwartz Phone 2 based on the following: (1) subscriber information provided by AT&T which indicates the phones are subscribed to Nelix Inc. with a contact name of SCHWARTZ and user address of Schwartz Residence 1; (2) police department records listing Schwartz Phone 1 as a phone belonging to SCHWARTZ; (3) information provided by Victim A indicating SCHWARTZ utilized the phones to contact Victim A; and (4) records obtained by Burner, a mobile application that allows users to create disguised phone numbers, indicating a number of Burner phone numbers that sent threatening text messages to Victim B were created by a user who provided Schwartz Phone 1 as the user's phone number. Based on these facts and my training and experience, it is likely that **SCHWARTZ** is the user of the phones and thus that his fingerprints are among those that are able to

⁸ <https://support.apple.com/guide/iphone/set-up-touch-id-iph672384a0b/ios> (last visited April 5, 2021).

⁹ <https://support.apple.com/en-us/HT209183> (last visited April 5, 2021).

unlock the phones via Touch ID and that his face will be able to unlock the phones via Face ID.

88. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers.¹⁰ In the event that law enforcement is unable to unlock the phones within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

89. Due to the foregoing, if Schwartz Phone 1 and Schwartz Phone 2 may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of MATTHEW SCHWARTZ, to the fingerprint scanner of Schwartz Phone 1 and Schwartz Phone 2; and (2) hold Schwartz Phone 1 or Schwartz Phone 2 in front of MATTHEW SCHWARTZ's face and activate the facial recognition feature for the purpose of attempting to unlock the phones in order to search the contents as authorized by this warrant.

¹⁰ Law enforcement will select the fingers to depress to the Touch ID sensor to avoid compelling the user of the device to disclose information about his or her knowledge of how to access the device.

IV. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

90. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

91. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

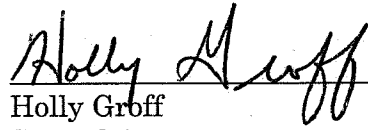
d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

92. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

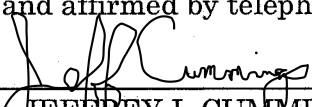
V. CONCLUSION

92. Based on the above information, I respectfully submit that there is probable cause to believe that the **Subject Offenses** have been committed, and that evidence, instrumentalities and contraband relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Premises**, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for the single-family home located at 1511 Guthrie Drive, Inverness, Illinois, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.


Holly Groff
Special Agent
Federal Bureau of Investigation

Sworn to and affirmed by telephone 20th day of May, 2021


Honorable JEFFREY I. CUMMINGS
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The two-story single family home with beige tiles on the first floor and white painting on the second floor with a front entrance with two white columns on either side of the front door and a circular driveway, as depicted below.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities and contraband concerning violation of Title 18, United States Code, Sections 875(c), 2261A, 1591, 2422, 2252 and 2252A, as follows:

1. Images of child pornography as defined in 18 U.S.C. § 2256(8).
2. Items in any format or medium, hidden or otherwise, that are capable of recording, capturing and/or storing video or images including but not limited to laptop computers, desktop computers, remote storage, and online storage .
3. Documents or other items concerning occupancy or ownership of the **Subject Premises**.
4. Documents or other items that demonstrate the use, ownership, or control of the electronic devices located at the **Subject Premises**, including the times any electronic devices were accessed, sales receipts, bills for internet access, and handwritten notes.
5. Items pertaining to or relating to financial transactions relating to the **Subject Offenses**.
6. Documents or other items that relate to contact with Minor A, other minors, victims of sex trafficking or witnesses.
7. Documents or other items that relate to contact with Individual A, including any threatening communications.

8. Cellular telephone bearing phone number (847) 682-6054 (Schwartz Phone 1).
9. Cellular telephone bearing phone number (224) 520-1591 (Schwartz Phone 2).
10. All other cellular telephones.¹¹
11. Weapons, including firearms.

¹¹ To the extent law enforcement locates phones in addition to Schwartz Phone 1 and Schwartz Phone 2, Attachment B authorizes only the seizure of these additional phones to allow law enforcement to preserve the phones and prevent destruction of evidence. The government will apply for additional warrants for any other seized telephones it seeks to search within one week of the phones' seizure, or else return the phones.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.